第 28 卷第 2 期　　四川理工学院学报(自然科学版)　　Vol. 28　No. 2
2015 年 4 月　　Journal of Sichuan University of Science & Engineering(Natural Science Edition)　　Apr. 2015
文章编号:1673-1549(2015)02-0014-04　　DOI:10.11863/j.suse.2015.02.04

两种抗时间片的攻击方法

姜海芳[a], 王海沛[b], 杨　威[a]

(成都信息工程学院 a. 应用密码学研究所; b. 信息安全工程学院, 成都　610225)

摘　要:针对插入时间片造成功耗曲线不能对齐,最终造成 CPA 攻击失败的情况,提出了两种解决方法:POC 和时-频转换。POC 方法利用相位计算功耗曲线间的波峰位置,得到功耗曲线间的偏移量,根据偏移量将功耗曲线进行对齐。时-频转换方法将时域的实测功耗通过频谱变换,换转成频域的功耗。以 SIC90C58AD 微控制器为硬件仿真平台,SM4 算法为研究对象,对加入了随机时间片的功耗曲线进行 POC 和时-频转换处理,并进行相关功耗分析攻击,结果显示:使用 POC 方法,197 条功耗曲线可以成功获取 SM4 密码算法的第一轮轮密钥;使用时-频转换方法,439 条功耗曲线可以获取密钥。证明 POC 和时-频转换方法可以对抗时间片。

关键词:相关功耗分析;时间片对抗;时-频变换;POC

中图分类号:TB115　　**文献标志码**:A

引　言

旁路攻击(Side Channel Attack,简称 SCA)作为一类新型的密码分析技术,已经得到了密码学界的广泛关注。相关功耗分析攻击[1](Correlation Power Analysis,简称 CPA)是一种典型的旁路攻击技术,其通过分析加密过程中密码芯片所产生的功耗与运算期间某些中间值的相关性达到破解算法密钥的目的。由于 CPA 是时域信号,因此要求采集的时域信号必须精确对齐,若所攻击的嵌入式加密系统中插入了随机时间片操作,由于各条功耗曲线相同操作时间点不对齐,加密系统处理不同功耗曲线的功耗差异不能在大量采集样本中得到累积,即使是对应正确密钥段的曲线也不会出现明显的尖峰,因此 CPA 无法攻破插入了随机延时的加密嵌入式系统。针对通过插入随机时间片造成 CPA 攻击失败的问题,本文提出了两种方法:

时-频转换和相位相关法(Phase-Only Correlation,简称 POC),以此破解插入随机时间片的密码系统。

1　随机时间片原理介绍

功耗攻击可以通过监测密码设备中的功耗来获得设备中的密钥,而这些泄露信息往往具有时间敏感性。敏感性体现在正常信号的尖峰出现在固定的时刻。针对这一特点,采用时间片对抗方法,在加解密过程中,通过人为在原有密码算法中插入随机长度的延时,可以提高采样复杂度和分析难度。由于每次加密操作是同一运算,每次运算的尖峰会出现在同一时刻,而插入随机时间片后,如图 1 所示(图 1 为 3 条插入了随机时间片的功耗曲线),将会造成时间点偏离,会造成功耗攻击失败。

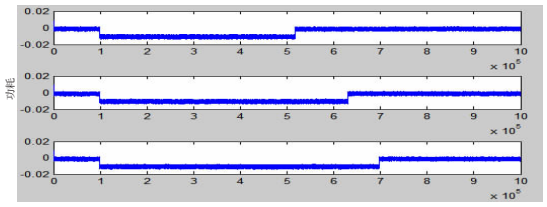

图 1　插入随机时间片的功耗曲线

收稿日期:2014-12-27

作者简介:姜海芳(1989-),女,河南鹤壁人,硕士生,主要从事旁路攻击与防护方面的研究,(E-mail)1659929293@qq.com

2　相关功耗分析攻击(CPA)分析

CPA 通过计算真实能量消耗值和假设能量消耗值之间的相关性来确定正确的密钥。h 表示假设功耗,t 表示实际功耗。其中 h 为 $D \times K$ 矩阵,t 为 $D \times T$ 矩阵,计算 h 的每一列和 t 的每一列的相关系数。计算时,使用相关系数 $r_{i,j}$ 表示列 h_i 和列 t_j 之间的线性关(其中,$i = 1,2,3,\cdots,K; j = 1,2,3,\cdots T$),$r_{i,j}$ 构成了一个相关系数矩阵 R,$r_{i,j}$ 表示相关系数矩阵 R 中第 i 行第 j 列元素,R 的尺寸为 $K \times T$。按照式(1)计算相关系数[2]:

$$r_{i,j} = \frac{\sum_{d=1}^{D}(h_{d,i} - \bar{h}_i) \cdot (t_{d,j} - \bar{t}_j)}{\sqrt{\sum_{d=1}^{D}(h_{d,i} - \bar{h}_i)^2 \cdot \sum_{d=1}^{D}(t_{d,j} - \bar{t}_j)^2}} \quad (1)$$

$$i = 1,2,3,\cdots,K; j = 1,2,3,\cdots,T$$

得到一个 $K \times T$ 的矩阵 R,它的每一个元素 $r_{i,j}$ 包含了 h_i 和 t_j 的比较结果,$r_{i,j}$ 越大说明 h_i 和 t_j 的匹配度越高,也就说明假设的密钥更接近于真实的密钥,找到矩阵 R 中的最大值,并把该值对应行的猜测作为正确的密钥猜测,该最大值揭示了对所选中间值进行处理的结果以及攻击设备所使用的密钥[3]。

3　抗时间片方法分析与介绍

对于插入了随机时间片的功耗曲线先进行 POC 或时 - 频转换操作,然后再进行 CPA 分析攻击,下面分别对两种方法进行介绍。

3.1　POC 分析

在对密码算法进行加密时,如果插入随机时间片,就会使功耗曲线产生位移误差,信息损失,造成功耗攻击失败[4]。然而,POC 可以利用相位相关法[5]将功耗曲线对齐,使功耗分析攻击可以成功进行。如果要实现功耗曲线对齐,就需要计算出各条功耗曲线的时间偏移量,POC 基于傅里叶变换的思想,通过计算波峰位置来确定偏移量。设 $f(n)$ 和 $g(n)$ 为长度相同的功耗曲线,w 表示 $f(n)$ 与 $g(n)$ 功耗曲线的偏移量,$n \in [-M, M]$。先对 $f(n)$ 和 $g(n)$ 进行离散傅里叶变换:

$$F(k) = \sum_{n=-M}^{M} f(n) W_N^{kn} = A_F(k) e^{j\theta_F(k)} \quad (2)$$

$$G(k) = \sum_{n=-M}^{M} g(n) W_N^{kn} = A_G(k) e^{j\theta_G(k)} \quad (3)$$

其中,$W_N = e^{-j\frac{2\pi}{N}}$、$A_F(k)$ 和 $A_G(k)$ 是振幅的不同表示方式,$e^{j\theta_F(k)}$ 与 $e^{j\theta_G(k)}$ 表示相位。根据式(4) ~ (5)计算 POC:

$$R(k) = \frac{F(k)\,\overline{G(k)}}{|F(k)\,\overline{G(k)}|} = e^{j\frac{2\pi}{N}k\delta} \quad (4)$$

$$POC = \frac{1}{N}\sum_{-M}^{M} R(k) W_N^{-kn} = \frac{\alpha}{N}\frac{\sin\{\pi(n+\delta)\}}{\sin\{\frac{\pi}{N}(n+\delta)\}} \quad (5)$$

其中 $\overline{G(k)}$ 是 $G(k)$ 的共轭。如果 $f(n)$ 和 $g(n)$ 相似,那么 $R(k)$ 会有很大的尖峰,尖峰代表了两条功耗曲线的相似性,尖峰对应的横坐标表示两条功耗曲线的偏移量。POC 具体操作方法:先选一条曲线作为基准曲线,然后计算其它功耗曲线和基准曲线的 POC,根据 POC 得到对应的尖峰值 $peak$,$peak$ 即为功耗曲线间的偏移量,根据每条功耗曲线的偏移量进行调整。所有功耗曲线调整完后,即可实现曲线的对齐,虽然 POC 可以精确地计算出偏移量,但是它只能处理在加密开始或结束时插入的时间片,对在加密轮次之间插入的时间片作用很小。

3.2　时 - 频转换分析

频谱(幅度谱和相位谱)是在频域中描述信号特征的方法之一,它反映了信号所含各分量的幅度和相位随频率的分布状况。时-频转换分析方法不同于 POC 分析方法,它打破了传统时域攻击的分析思路,从频域的角度出发,根据信号在时域上的幅度变化将导致此信号在频域上产生同样的幅度变化[6]这一特点,将时域的实测功耗通过频谱变换,转换成频域的实测功耗,丢掉相位信息,只保留幅度信息,能够很好地解决功耗曲线未对齐问题[7-8]。

有限长序列 $x(n)(0 \leqslant n \leqslant N-1)$ 经傅里叶变换后为 $X(k)$:

$$X(k) = FFT[x(n)] = \sum_{n=0}^{N-1} x(n) W^{nk} (0 \leqslant k \leqslant N-1)$$

$$W = e^{-j(\frac{2\pi}{N})}$$

由傅里叶特性[9]可知:若 $DFT[x(n)] = X(k)$,$y(n) = x(n-m)R(n)$,则:

$$DFT[y(n)] = W^{mk} X(k)$$

这表明信号 $x(n)$ 在时域中时移 m 位,频域中其 DFT 乘以相移因子 W^{mk},也就是说信号时移后,幅度谱不变,相位谱发生变化。现假设实测功耗曲线数量为 n,每条功耗曲线的长度为 N,则功率谱密度为:

$$Tpsd(i) = \frac{1}{N}|FFT(x(i))|^2$$

则 $\{Tpsd(1), Tpsd(2), Tpsd(3), \cdots Tpsd(number)\}$ 为一条功耗曲线的各个功耗点的功率谱密度,i 为功耗点。

详细攻击过程可参考文献[2]。

4 攻击实验与结果

实验使用硬件环境如图 2 所示。PC 机将 128 位随机明文,通过串口发送至 STC90C58AD 单片机。STC90C58AD 单片机收到明文后运行 SM4 加密程序,利用存储在其中的密钥对明文进行加密。同时 STC90C58AD 单片机引脚生成的触发信号触发 TekDPO4032 示波器对电阻 R 上的电压进行采样并存储,进而通过以太网总线将数据上传至 PC。STC90C58AD 单片机利用串口将密文发送至 PC,应用程序将明文、密文、对应的电压采样数据进行保存。利用明文、功耗曲线进行 CPA 攻击,其中明文样本量分别为 250(POC 方法)、500(时-频转换方法),采样深度为 30 000 点,采样频率为 250 M/s。产生的功耗曲线样本量分别为 250 条(POC 方法)、500 条(时-频转换方法)。

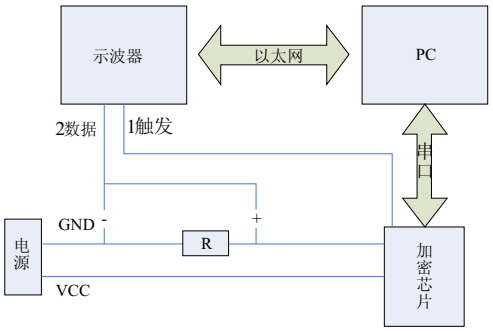

图 2 实验使用的硬件环境

首先对插入时间片的功耗曲线,进行 POC 操作,然后进行 CPA 功耗分析攻击,图 3 为攻击结果图,从图中可以看出随着功耗曲线的增加,CPA 的攻击成功率逐渐上升,当功耗曲线的条数增加到 197 条时,破解密钥的成功率达到 100%,成功破解 SM4 算法的第一轮密钥,表 1 给出了猜测正确时第一轮 4 个密钥字节对应的相关系数值以及对应的功耗曲线的样本点。

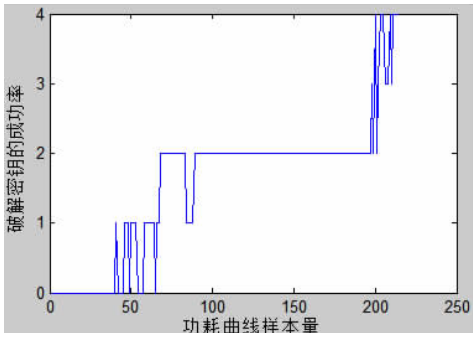

图 3 功耗曲线样本量与破解成功率的关系(POC)

表 1 POC 攻击的精确相关系数

第一轮 4 个字节	第一个字节	第二个字节	第三个字节	第四个字节
相关系数	0.249017	0.238072	0.253702	0.263524
样本点	75	129	69	133

对于时-频转换方法,同样通过实验进行验证,即首先插入时间片的功耗曲线进行时-频转换操作,然后进行 CPA 攻击。图 4 为攻击结果图,从图中可以看出随着功耗曲线的增加,CPA 的攻击成功率逐渐上升,当功耗曲线的条数增加到 439 条时,破解密钥的成功率达到 100%,成功破解 SM4 算法的第一轮密钥,表 2 给出了猜测正确时 4 个密钥字节对应的相关系数值以及对应的功耗曲线的样本点。

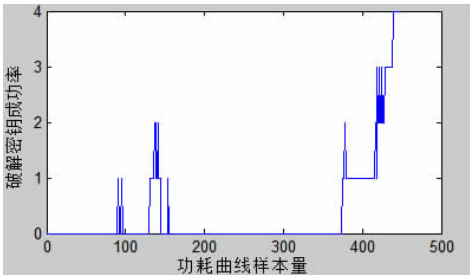

图 4 功耗曲线样本量与破解成功率的关系(时-频转换)

表 2 时 – 频转换攻击的精确相关系数

第一轮 4 个字节	第一个字节	第二个字节	第三个字节	第四个字节
相关系数	0.269242	0.238195	0.253949	0.280471
样本点	75	130	65	133

使用时 – 频转换方法,整个攻击过程需要 1756 秒,破解密钥所需的功耗曲线所占的空间大小为 155 M。使用 POC 方法,整个攻击过程需要 1056 秒,功耗曲线所占的空间大小为 65 M。从时间、空间上可以看出,POC 方法效率高,但是 POC 方法具有局限性,因为 POC 是将没有对齐的功耗曲线进行对齐,而对齐方法只能对加密开始或结束插入随机时间片的功耗曲线进行对齐,对在加密轮次之间插入随机时间片的功耗曲线无能为力;而时 – 频转换方法没有局限性,因为它是将时域的实测功耗通过频谱变换,换转成频域的实测功耗,在频域方面,插入时间片是不起作用的。

5 结束语

本文针对时间片防御方法造成的功耗曲线不能对齐、相关功耗攻击不能成功的情况,提出了两种攻击方法:POC 和时-频转换方法,并以 SIC90C58AD 微控制器为硬件仿真平台,SM4[10] 算法为研究对象,对这两种方法进行实验验证,实验结果表明:通过使用 POC 方法,

197 条功耗曲线可以成功获取 SM4 密码算法的第一轮轮密钥;通过使用时-频转换方法,439 条功耗曲线可以成功获取 SM4 密码算法的第一轮轮密钥。证明了 POC 和时-频转换方法的有效性,另外 POC 方法攻击需要的功耗曲线数量明显少于时-频转换方法,说明 POC 的攻击效率高于时-频转换方法。

参 考 文 献:

[1] Brier E,Clavier C,Olivier F.Correlation power analysis with a leakage model[C]//Proceedings of the 6th International Workshop on Cryptographic Hardware and Embedded Systems (CHES2004), Boston, USA, 2004:135-152.

[2] Stefan M,Elisabeth O,Thomas P.能量分析攻击[M].北京:科学出版社,2010.

[3] 罗晓飞,陈运,陈俊,等.针对 DES 密码芯片的两种功耗攻击对比分析[J].成都信息工程学院学报,2012,27(6):536.

[4] 王创伟,张西红,李永浩,等.基于时间延迟和掩码的抗 DPA 方法研究[J].计算机测量与控制,2011,19(11):2801.

[5] Zhang L, Zhang D. Finger-knuckle-print verification based on bandlimited phase-only correlation[C]//Proceedings of the 13th International Conference on Computer Analysis of Images and Patterns. Berlin:Springer Verlag, 2009:141-148.

[6] Steven W S.The scientist and engineer's guide to digital signal processing[M]. California:California Technical Publishing,2003.

[7] 黄永远,陈运,陈俊,等.运用频域辅助分析的 AES 算法相关功耗攻击[J].四川大学学报:自然科学版,2014,51(3):459.

[8] 黄永远,陈运,陈俊,等.针对 AES 算法的时域和频域相关功耗攻击对比分析[J].成都信息工程学院学报,2013,28(5):460.

[9] Chari S,Rao J R,Rohatgi P.Template attacks[C]//Cryptographic Hardware and Embedded Systems-CHES 2002.Springer Berlin Heidelberg,2003:13-28.

[10] 国家商用密码管理办公室.无线局域网产品使用的 SMS4 密码算法[EB/OL]. (2006-01-06). http://www.ossca.gov.cn/news/200709/news_1105.htm

Two Attack Methods Against the Time Slices

JIANG Haifang[a], *WANG Haipei*[b], *YANG Wei*[a]

(a. Applied Cryptography Institute; b. School of Information Security Engineering, Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: Inserting random time slices in the power curve will cause the power curve unable to be aligned, which resulting in CPA attacking failure. In view of this case, two solutions are put forward: POC and time-frequency conversion. POC method uses the knowledge of phase to compute the position of power curves' wave peak, the offset between power curves is obtained. And the power curves are aligned according to the offset. In time-frequency conversion method, the measured power consumption of time domain is changed to the power consumption of frequency domain by spectrum transform. Taking the SIC90C58AD micro controller as hardware simulation platform, SM4 algorithm as the research target, the power curves which have been inserted with random time slices are dealt by using POC and time-frequency conversion, and disposed with correlation power analysis attacking, the experimental results show: with using of POC method, 197 power traces can successfully acquire SM4's first round keys; with using of time-frequency conversion method, 439 power traces can acquire the keys. It is proved that the POC and time-frequency conversion can successfully attack the time slices.

Key words: correlation power analysis(CPA); time slices countermeasure; time-frequency conversion; POC